Security Bulletin for Directory Traversal Vulnerability in MiCollab AWV

SECURITY BULLETIN ID: 20-000-01

RELEASE VERSION: 1.0

DATE: 2020-05-01

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 20-0005-01. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address the Directory Traversal vulnerability found in MiCollab AWV conference URL.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiCollab	MiCollab 8.1.2 and earlier And 9.1.2 and earlier	Upgrade to MiCollab 8.1.2.4, Upgrade to MiCollab 9.1.3 or later

RISK / EXPOSURE

Directory Traversal Vulnerability (CVE-2020-11798)

A Directory Traversal vulnerability in web conference component of MiCollab AWV could allow an attacker to access arbitrary files from restricted directories of the server using a specially crafted URL due to insufficient access validation. A successful exploit could allow an attacker to access sensitive information from the restricted directories and impact confidentiality of the data.

The risk due to this vulnerability is rated as MEDIUM.

	CVSS v3.0	CVSS v2.0
CVSS OVERALL SCORE:	7.3	7.5
CVSS VECTOR:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS BASE SCORE:	7.3	7.5
CVSS TEMPORAL SCORE:	Not Defined	Not Defined
CVSS ENVIRONMENTAL SCORE:	Not Defined	Not Defined
OVERALL RISK LEVEL:	Medium	Medium

Mitel
Powering connections

MITIGATION / WORKAROUNDS

Customers with affected product versions should upgrade to the highlighted solution versions or later.

SOLUTION INFORMATION

These issues are addressed in MiCollab 8.1.2.4 and MiCollab 9.1.3.

Customers are advised to upgrade to these releases. Please contact Product Support for more information.